UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,884	03/03/2000	George Fleming	US008002	5479

7590 02/23/2005

U S Philips Corporation
Corporate Patent Counsel
580 White Plains Rd
Tarrytown, NY 10591

EXAMINER
ADAMS, JONATHAN R

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/517,884	FLEMING ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The following rejection has been entered into the record, and has been modified from the previous rejection to place it in better condition for appeal.

Claim Rejections - 35 USC § 102

In view of the appeal filed on 8/18/04, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7, and 12 rejected under 35 U.S.C. 102(b) as being anticipated by Abraham et al., US Patent No 5148481 (hereafter referred to as '481).

As to claim(s) 1:

'481 teaches a processing system comprising:

- Application device configured to communicate information with a physical layer access device via a link layer access device / security functions relating to the IC card (Physical layer access device) or card reader are requested by the customer application program (run on processor 13/Application device), pass down through the various program interfaces through cryptographic adapter (link layer access device) to card reader (Col 7, Lines 53-56, '481).
- Node controller that is configured to control the link layer access device / Security functions (Col 7, Lines 53-56, '481) / device driver (Col 7, Lines 53-56, '481)
- Link layer access device coupled to application device, node controller and physical-layer access device / Configured to facilitate an exchange of information from and to the application device with data that is communicated to and from the physical layer access device / security functions relating to the IC card (Physical layer access device) or card reader are requested by the customer application program (run on processor 13/Application device), pass down through the various program interfaces through cryptographic adapter (link layer access device) to card reader (Col 7, Lines 53-56, '481).

- Link layer access device configured to provide one or more cryptographic items based on one or more based on parameters and commands from node controller / Keys are stored in cryptographic adapter (Col 7, Line 48-50, '481), The IWS may utilize only the cryptographic adapter card 29, into which user authorization profiles are downloaded from the host computer and in which high-speed cryptographic functions such as application program encryption are performed. (Col 4, Lines 4-10, '481)

As to claim(s) 2, 3:

Cryptographic items include cryptographic key item / Security server program 117 provides the program modules and information, the cryptographic keys needed to perform a specific function, to the cryptographic adapter hardware 29 through a device driver program 119. Example program modules include key management module 121 message authentication code verification 123, message authentication code generator 125, and encypher/decypher functions 127, 129. (Col 7, Lines 34-39, '481)

As to claim(s) 5:

Node controller is configured to effect an exchange of a cryptographic key with an other processing system / When the user inserts the user's IC card, step 325, into the IC card read/write unit 17, those two devices establish a secure session between them

in step 327. This action occurs transparently to the user, is built on the existence of a cryptographic processor in both devices, and results in a unique session key (Col 14, Lines 15-20, '481)

The one or more cryptographic items from the link layer access device includes the cryptographic key / Security server program 117 provides the program modules and information, the cryptographic keys needed to perform a specific function, to the cryptographic adapter hardware 29 through a device driver program 119. Example program modules include key management module 121 (Col 7, Lines 34-39, '481)

As to claim(s) 7:

- Application-layer interface device configured to communicate information with an application layer device / Physical-layer interface device configured to communicate with a physical layer device / Buffer device operably coupled to application layer interface device and physical layer interface device / Configured to facilitate exchange of information of application layer device and physical layer device/ Security functions (Application-layer interface device) relating to the IC card (Physical layer device) or card reader (physical layer interface device) are requested by the customer application program (run on processor 13/ application layer device), pass down through the various program interfaces (buffer device) through cryptographic adapter (accelerator) to card reader (Col 7, Lines 53-56, '481).

- Controller interface device coupled to application layer interface device and physical layer interface device facilitates control of exchange of information and data / device driver (Col 7, Lines 53-56, '481), (Fig 5, Element 119, '481)
- Accelerator coupled to controller via controller interface device configured to compute one or more cryptographic items in response to one or more cryptographic commands from the controller / Keys are stored in cryptographic adapter (Col 7, Line 48-50, '481), The IWS may utilize only the cryptographic adapter card 29, into which user authorization profiles are downloaded from the host computer and in which high-speed cryptographic functions such as application program encryption are performed. (Col 4, Lines 4-10, '481)

As to claim(s) 12:

Claim 12 corresponds to claim 1 and 7

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 6, 8, 11, 15, 17 rejected under 35 U.S.C. 103(a) as being unpatentable over '481 in view of Sutikno "Design and Implementation of Arithmetic Processor F_2^{155} for Elliptic Curve Cryptosystems"

As to claim(s) 4, 8, and 15:

Abraham et al discloses the processing system of claim 1, but fail to show that it includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller. Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-4 1 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others. Sutikno also teaches deriving a second point from the first point on the elliptic curve is a function in ECC (Sutikno, col. 2, line 18, specifically the equation) from inputs (one or more of the parameters) (Sutikno, col. 5, lines 30-33) and where the Main Controller controls all the process to the of the arithmetic processor (Sutikno, col. 7, line 7-9). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutikno to include the benefits of having a ECC coprocessor in the node controller because of the small area and the flexibility of the arithmetic processor making it suitable for IC card applications (Sutikno, col. 8, line 8- I 0).

As to claim(s) 6, 11, and 17:

Abraham et al discloses the processing system of claim 1 however fail to show that the commands from the node controller include:

- a basepoint multiply command,
- a point multiply command,
- an EC-DSA verify command, and
- an EC-DSA sign command.

In regards to multiply commands and EC-DSA commands, Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-41 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutïkno to include the benefits of having a ECC coprocessor in the node controller because of the small area and the flexibility of the arithmetic processor making it suitable for IC card applications (Sutikno, col. 8, line 8- 10).

Response to Arguments

Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

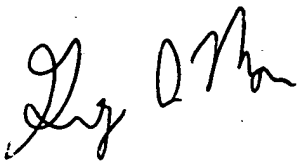
Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (571)272-3832. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (571)272-3838. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100